UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/783,112	02/14/2001	Josh N. Hogan	10971806-3	2220

7590   11/10/2004

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/783,112	HOGAN, JOSH N.
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 July 2004*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
    closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,10 and 26-28* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 10, and 26-28* is/are rejected.

7)☐ Claim(s) _ _ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
        application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)   4)☐ Interview Summary (PTO-413)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)   Paper No(s)/Mail Date. _____ .
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)   5)☐ Notice of Informal Patent Application (PTO-152)
   Paper No(s)/Mail Date _____.   6)☐ Other: _____.

1.   This Action is in response to Applicant's correspondence dated 27 July 2004.

2.   The arguments for rejection of claims 1, 10, and 26-28 that were presented in the

previous Action have been withdrawn. However, Examiner has drawn new grounds for

rejection for the pending claims. Applicant's arguments have been considered, but are

found to be moot in view of the new grounds for rejection.

3.   Claims 1, 10, and 26-28 are pending.

Double Patenting

4.   The nonstatutory double patenting rejection is based on a judicially created
doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the
unjustified or improper timewise extension of the "right to exclude" granted by a patent
and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11
F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225
USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA
1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*,
418 F.2d 528, 163 USPQ 644 (CCPA 1969).
        A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be
used to overcome an actual or provisional rejection based on a nonstatutory double
patenting ground provided the conflicting application or patent is shown to be commonly
owned with this application. See 37 CFR 1.130(b).
        Effective January 1, 1994, a registered attorney or agent of record may sign a
terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with
37 CFR 3.73(b).

5.   Claims 1 and 26 are rejected under the judicially created doctrine of

obviousness-type double patenting as being unpatentable over claim 8 of U.S. Patent

No. 6,252,961. Although the conflicting claims are not identical, they are not patentably

distinct from each other because the patent claim recites every element from the claims

of the instant application except for two details. With regards to the ECC block that is

coded according to an error code correction method, this element is a tautology that

adds no new matter over the claim in the instant application; a block of ECC-coded data must, by definition, be encoded according to an error code correction method. With regards to the encryption mask being encoded according to the same error code correction method, note that the patent teaches that the disclosed system would function correctly even if the encryption mask contained errors (Hogan, column 5, lines 60-63). Therefore, it would have been obvious to one of ordinary skill in the art to omit this step, as it would not disrupt the functioning of the remaining elements while simplifying the overall design. *In re Karlson* 136 USPQ 184 (CCPA 1963)

6.   Applicant is advised that should claim 1 be found allowable, claim 26 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 102

7.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8.   Claims 27 and 28 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the

alternative, under 35 U.S.C. 103(a) as obvious over Winkler et al. (U.S. Patent

5,594,862), and as appropriate in view of Schneier ("Applied Cryptography, 2nd edition",

©1996).

Winkler discloses an XOR controller (Winkler, element 23 of Figure 1). The

invention also possesses a microprocessor that can read data from multiple sources

and load it into the controller's cache memory (Winkler, column 2, lines 8-13). As part

of its normal function, the controller uses blocks of parity data (Winkler, column 3, lines

38-41), parity being a technique for ECC encoding that is well known in the art. The

XOR controller takes two blocks of data (D_{old} and D_{new}) and one block of parity data

(P_{old}) and performs a bitwise XOR arithmetic operation on them, resulting in an

encrypted parity block (Winkler, column 5, lines 21-33). It should be noted that due to

the associative property of bitwise XOR arithmetic, the quantity ($D_{old} \oplus D_{new}$) is

equivalent to an encryption mask; a Boolean truth table that supports this assertion can

be supplied upon request. If Applicant contends that the result of the XOR controller is

not an encrypted parity block, then it can be seen as an obvious development in light of

the teachings of Schneier. Schneier relates that in the general case the XOR arithmetic

operation is functionally equivalent to a Vigenère polyalphabetic cipher (Schneier,

pages 13-15, particularly 1st paragraph of page 14). Therefore, it would have been

obvious to one of ordinary skill in the art to view the existing function of the XOR

controller disclosed in Winkler as an encryption device, as one would gain the ability to

protect data, however limited, on a storage device.

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

10.   Claims 1, 10, and 26 have been rejected under 35 U.S.C. 103(a) as being

unpatentable over the combination of Davis (U.S. Patent 5,825,879), Monroe et al. (U.S.

Patent 5,293,388), Barnes et al. (U.S. Patent 4,172,213), Schneier ("Applied

Cryptography, 2nd edition", ©1996), Poggio ("CD-ROM Technical Specification", April

1988) and Applicant Admitted Prior Art (henceforth AAPA).

Regarding claims 1 and 26, Monroe teaches a system comprising: a computer

bus (Monroe, element 20 of Figures 1-3, and also column 1, lines 17-25); a host

processor connected to the computer bus (Monroe, element 80 of Figure 3) that is

programmed to perform error code correction (Monroe, column 7, lines 62-64); a

peripheral drive constituting the means by which ECC encoded data is supplied to the

processor (Monroe, column 1, lines 44-57 and also elements 50 and 50A of Figure 3).

As noted in a prior Action, Monroe is silent regarding any potential encryption of the

data read from the device.

Davis discloses a system for protecting video content that includes a Secure

Video Content Processor (Davis, elements 20 and 28 of Figure 2). It also contains

features akin to those possessed by the invention disclosed by Monroe, including a host

processor, disk controller, protected data, and a data bus (Davis, elements 104, 108,

120, and 128 respectively). The SVCP contains circuitry for further encryption of data

that has been read from the disk (Davis, element 424 of Figure 4 and also column 6,

lines 5-9). The encryption circuitry clearly contains frame data keys, which are

functionally equivalent to the encryption mask proposed by Applicant (Davis, column 5,

lines 32-39). It should also be noted that in an alternate embodiment of the invention

disclosed by Davis, the SVCP can be built in to DVD and CD-ROM drives (Davis,

column 7, lines 19-20). Therefore, it would have been obvious to one of ordinary skill in

the art at the time the invention was made to incorporate the encryption capabilities

found in the particular embodiment of Davis above into the invention disclosed by

Monroe. Adding encryption in this manner helps remedy a known deficiency in prior art

attempts to secure digital content (Davis, column 2, lines 1-4).

Applicant has remarked that Davis does not teach that the source data has been

ECC encoded prior to encryption. Davis does teach that the source can be a DVD or

CD-ROM (Davis, column 7, lines 19-20); further, Applicant is reminded of his admission

that DVD and CD players inherently contain error correction capabilities (AAPA, page 1,

lines 19-23). In addition, Poggio teaches that all data encoded on a CD-ROM must

necessarily be ECC-encoded as part of the specification (Poggio, page 5, "Second

Level Error Correction"). Therefore, it would have been obvious to one of ordinary skill

in the art at the time the invention was made to embody the combination of Monroe and

Davis in such a way that it would obtain its source data from a CD that was ECC-

encoded, as admitted by Applicant and Poggio. Error correction technologies help

ensure a positive user experience by compensating for any physical defects in the disc

or noise on the read channel (AAPA, page 1, lines 15-18).

None of the cited references teach the method of XOR encryption as the

particular form of encryption used. However, Barnes teaches an encryption system

which can selectively encrypt and decrypt data without modifying control commands

and communications protocols (Barnes, column 2, lines 31-39). The encryption

involves executing an XOR operation on both a key and a plaintext to produce a cipher

(Barnes, column 6, lines 1-4; all of Figure 1; and element 7-32 of Figure 7). Applicant

should take heed that Barnes teaches that the XOR encryption used here can also be

used as a form of data authentication, whereby a cryptographic checksum is generated

from plaintext to be used by the receiver to verify that the plaintext message was

received exactly as it was sent (Barnes, column 7, line 53 to column 8, line 20). This

functionality is clearly analogous to error correction; further, no additional hardware

would be required to gain this additional functionality. Therefore, it would have been

obvious to one of ordinary skill in the art at the time the invention was made to use XOR

based encryption as disclosed in Barnes as the method of encryption used in the

combination of Monroe, Davis, Poggio, and AAPA, for the aforementioned reason.

Regarding claim 10, again note that, with regards to the combination of

references cited above, any data encrypted by an XOR processor as found in Barnes

will be sent to the host processor as found in Monroe for further ECC processing

(Monroe, column 7, lines 62-64; and Barnes, column 2, lines 31-39).

Oath/Declaration

11.   Applicant's remarks regarding Examiner's prior objection to the declaration have

been noted. Applicant is respectfully reminded to correct the following aspects of the

declaration:

> It does not state that the person making the oath or declaration has reviewed and
> understands the contents of the specification, including the claims, as amended
> by any amendment specifically referred to in the oath or declaration.

> It does not state that the person making the oath or declaration acknowledges
> the duty to disclose to the Office all information known to the person to be
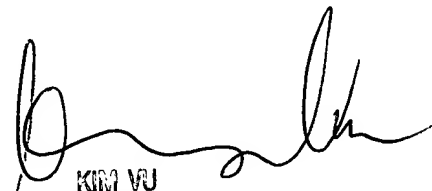> material to patentability as defined in 37 CFR 1.56.

Conclusion

12.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849.

The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

TAG
10/15/04

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100